Projects

Petra Manche

Create

- Projects
- Milestones
- Tasks
- Discussions
- Gantt Chart
- Time Tracking
- Documents
- Reports
- Project Templates
- Settings
- Help Center
- Feedback & Support

Marketing CC to non-Government Industries

Comments (2) | Subscribers (29) | Documents | Overview

Matthew Keller 8:00 AM 1/14/2016

During the last CCUF Workshop in the UK, the Marketing Working Group held a session and the discussions covered a range of ideas for marketing CC. It was clear from the discussions that the Marketing Group has many different potential audiences and the messages for those audiences vary greatly. The Marketing Group could spend effort to market CC to new nations to join the CCRA, to government End Users to increase the value of a CC certification, to companies in IT Security that are not currently using CC evaluation as a tool, and to new industries outside of the government sector.

I found the last potential audience mentioned above to be particularly interesting. Marketing the value of CC validated products to other industries would increase the potential ROI for all vendors pursuing a CC evaluation. I think there could be significant value to an non-government industry group from leveraging an entire existing evaluation program to provide assurance to purchasers. We need to be realistic in that any of these new industries may need custom SFRs or specific assurance requirements, but the current "tailored assurance" PPs that are being produced by iTC provide a lot of flexibility for using the CC to define new functional and assurance requirements that are needed.

The industries that were mentioned during the workshop were; Finance, Health Care, Automotive, and Monitoring and Sensors (IoTs). Many of these industries are at a crossroads where they understand the need for IT security in the products and services but they have not defined a widely used testing or assurance program to provide confidence in the IT security of products. Part of the discussion at the CCUF workshop focused on how the smart card industry achieved such success; with the purchasers understanding and requiring CC evaluation. In the smart card space, both the vendors and a central organizing body worked together to establish CC evaluation as a best practice and then as a hard requirement. Both parties realized that some common security requirements were necessary and the Common Criteria provided the tool they needed. I think it is likely that some of these new industries will see the same value in the CC evaluation program.

The existing Common Criteria standard, evaluation methodology, laboratory infrastructure, and cumulative experience with IT Security evaluations are a great value to an industry group trying to figure out how to provide assurance in the IT security of products. These non-government industries would not have to reinvent the wheel, they could leverage an entire existing testing and assurance program.

So the question I have for this group is what can we do to engage these industries and at least start the conversation about the benefits of a Common Criteria evaluation for product in their industry?

Matthew Keller 11:57 AM 1/14/2016

Is there anyone that is attending this conference or has an interest in attending this conference? If so, perhaps we can get some contacts from this conference or an idea of who we should start talking to.

Automotive IQ is bringing the 3rd Automotive Cyber Security Summit back to Detroit on March 21-23.

View Agenda>>> http://goo.gl/0TX0RK

It looks like there is some presentations around security in Automobile products.

Matthew Keller 12:06 PM 2/1/2016

There was an interesting discussion during the CCUF General Membership meeting on this topic. One lab representative mentioned that during discussions with auto makers and auto IT vendors, he felt the industry has acknowledged there is a problem with security of the products in the space right now. The industry as a whole seem to be looking for solutions for how to gain assurance in auto IT products. The lab also indicated that several of the problems the auto industry is facing right now are similar to network security issues that have already been seen and delta with in physical and WiFi network security.

I asked the large vendors on the CCUF call about attending auto IT conferences and waving the CC flag at the events. Many vendors do have someone attending these events but the attendees are from the sales or marketing side of the business and are not resources that are well versed in CC. Another hurdle is that discussing CC as a solution would not be the top goal for a marketing or sales representatives for how they spend their time there.

One large security product vendor said that many times there is fear from vendors about evangelizing for CC in markets other than government. If the market makes CC a best practice or a hard requirement, then there is another hurdle to sales in that market. However, the same vendor said, that hurdle could be a competitive advantage to the company. When the company is already seeking CC validation on products because of the government market, adding another industry that values or requires the CC validation just blocks other competitors that do not have CC.

How can we get the marketing and sales staff at companies that are already attending health IT, auto IT, or IoT security events to discuss the values of CC validation while they are at the events? Is there some tool we could provide them with?

Other than signing up to speaks about CC at a health IT security conference or an auto IT security conference, how can we engage with these others industries? Should we be looking to do whitepapers and blog posts about the how CC validation provides assurance and what the already existing CC validation infrastructure could bring to the health IT or auto IT industry?

Add Comment